ANALISIS STEGANOGRAFI VIDEO MENGGUNAKAN METODE *ENHANCED LEAST SIGNIFICANT BIT* PADA FRAME YANG TERDETEKSI *SILENCE* BERBASIS *DISCRETE WAVELET TRANSFORM*

Analysis of Video Steganography Using Enhanced Least Significant Bit on Frame with Silence Detection Based on Discrete Wavelet Transform

Wulandari Setiawati[1], Dr. Ir. Bambang Hidayat, DEA[2], I Nyoman Apraz Ramatryana, S.T.,M.T.[3]
Prodi Teknik Telekomunikasi Fakultas Teknik Elektro, Telkom University
wulan.setiawati9@gmail.com[1], avenir.telkom@gmail.com [2], ramatryana@gmail.com [3]

Abstrak

Penggunaan media internet untuk melakukan pertukaran informasi yang telah berkembang menyebabkan kekhawatiran terkait keamanan dan kerahasiaan data digital yang dikirimkan. Untuk mengamankan data yang dikirimkan melalui media internet, diperlukan suatu teknik agar keamanan dan kerahasiaan informasi tersebut terjamin, salah satunya yaitu Steganografi. Pada penelitian ini, dirancang sebuah sistem steganografi dimana pesan yang disisipkan berupa file citra RGB (*Red Green Blue*) berformat **.bmp* dan video dengan format *.avi sebagai cover. Pesan informasi disisipkan pada *frame* video berdasarkan deteksi *silence* menggunakan *Discrete Wavelet Transform*, dengan metode penyisipan yaitu ELSB. Proses pengujian keberhasilan Video Steganografi dilakukan dengan mengukur parameter seperti: PSNR, MSE, BER, dan MOS. Dengan menggunakan metode penyisipan ELSB didapatkan hasil *Peak Signal to Noise Ratio* (PSNR) yang baik. Hasil PSNR terbesar yaitu 68,7518 dB dan nilai MSE terkecil sebesar 0,00867. Waktu komputasi terbesar yang didapat pada proses penyisipan adalah 91,15508 detik, sedangkan pada proses ekstraksi adalah 76,71934 detik. Hasil *Mean Opinion Score* (MOS) yang didapatkan memiliki nilai rata-rata total sebesar 4,1764 yang berarti kualitas video tersisipi dengan baik. BER terbesar yang dihasilkan yaitu sebesar 0,901899 saat *mean* = 0 dan variansi = 0.5.

Kata kunci : Steganografi Video, *Silence Detection, Discrete Wavelet Transform, Enhanced Least Significant Bit.*

Abstract

*Usage of internet to exchange information that have been developed cause worries about security and privacy of digital data being transmitted. To secure the data sent via internet, a technique to guarantee the security and privacy is needed. One of the method is called Steganography. In this final assignment, a Steganography system is designed to embed *.bmp formatted RGB image to *.avi formatted video. The image is secret message, while the video is used as cover. The secret message is embedded by ELSB method to video frames based on silence detection with DWT method. The success rate of Video Steganography carried out by measuring several paramaeters, such as: PSNR, MSE, BER, and MOS. PSNR biggest result obtained is 68,7518 dB and MSE lowest result is 0,00867. Longest computational time in embedding process is 91,15508 second, while longest computational time in extraction process is 76,71934 second. MOS result have an average of 4,1764, meaning that the quality of the video after embedded with image is good. The resulting BER is equal to 0.901899 when the mean = 0 and variance = 0.5.*

Keywords: Video Steganography, Silence Detection, Discrete Wavelet Transform, ELSB.

1. Pendahuluan

Seiring dengan kemajuan teknologi, pertukaran informasi melalui media digital semakin sering dilakukan, dan menjadi aktivitas kebanyakan orang sehari-hari. Namun, tidak dapat dipungkiri bahwa kemajuan teknologi dan informasi selain memiliki banyak keuntungan, juga terdapat sisi negatif, misalnya seperti pencurian konten atau data digital yang dikirim melalui internet dapat disalahgunakan oleh orang yang tidak bertanggung jawab[9]. Penggunaan media internet untuk melakukan pertukaran informasi yang telah berkembang menyebabkan kekhawatiran terkait keamanan dan kerahasiaan data digital tersebut. Sehingga diperlukan suatu teknik untuk dapat bertukar informasi tanpa ada orang lain yang mengetahui kecuali orang yang bersangkutan. Teknik ini dinamakan Steganografi. Pada Tugas Akhir ini, dilakukan analisis dan simulasi teknik steganografi pada video, karena video merupakan gambar berjalan yang terdiri dari beberapa *frame* yang mampu menampung kapasitas yang lebih besar daripada gambar. Video menggunakan format *.*avi* yang tidak terkompresi dengan penyisipannya menggunakan metode *Enhanced Least Significant Bit.* Serta dilakukan dengan pemilihan *frame* pada video berdasarkan deteksi *silence* berbasis *Discrete Wavelet Transform*. Data rahasia yang akan disisipkan pada video berupa gambar dengan

format *.bmp*. Pada proses penyisipan gambar, dilakukan dengan menentukan daerah *silence* pada sinyal audio, yang merupakan titik acuan dalam melakukan penyisipan pesan rahasia pada *frame* video. Kemudian teks disisipkan pada *frame* video saat daerah *silence* terdeteksi. Performansi sistem diuji berdasarkan perhitungan *Mean Square Error* (MSE), *Peak Signal to Noise Ratio* (PSNR), *Bit Error Rate* (BER) dan *Mean Opinion Score* (MOS). Disamping itu, tingkat ketahanan stego-video ini diuji dengan *Gaussian Noise*.

2. Landasan Teori

2.1 Steganografi[9]

Steganografi berasal dari bahasa yunani yaitu *steganos* yang berarti tersembunyi atau menyembunyikan, sedangkan *graphy* berarti tulisan, sehingga secara keseluruhan artinya adalah tulisan yang disembunyikan. Teknik steganografi digunakan untuk menyembunyikan pesan rahasia ke dalam pesan lain. Pada umumnya terdapat dua proses di dalam steganografi, yaitu proses penyisipan pesan rahasia dan proses ekstraksi pesan untuk mendapatkan pesan rahasia dari dalam pesan tersebut.

Steganografi digital menggunakan *file-file* multimedia sebagai *cover*, misalnya citra, suara, teks, dan video. *Secret message* yang disembunyikan juga dapat berupa citra, suara, teks, atau video. *Stego Object* adalah *cover* yang telah disisipkan pesan rahasia[6].

2.2 Format .AVI[9]

Audio Video Interleave (AVI) adalah format *file* penyimpan data- data multimedia. AVI diperkenalkan pertama kali oleh *Microsoft* pada bulan November 1992 sebagai bagian dari teknologi video dalam *platform Microsoft Windows*. Format AVI merupakan salah satu format video tertua yang diperkenalkan *Microsoft* sejak dilirisnya *Windows* 3.1. Format *file* AVI dapat menyimpan data video dan audio dalam satu *file* yang memungkinkan memainkan kedua jenis data secara bersamaan. Dalam Tugas Akhir ini memakai AVI *uncompressed* atau disebut juga AVI *full frames*. Suatu file multimedia dengan format AVI *uncompressed* memiliki informasi *frame-frame* gambar yang disimpan dengan menggunakan format *Bitmap* tiga layer warna 8 bit, jadi untuk satu pixel data *bitmap* akan disimpan dalam wadah berukuran 24 bit.

2.3 Metode ELSB[4][7]

Enhanced Least Significant Bit merupakan modifikasi dari metode *Least Significant Bit*. Metode ini dapat dilakukan dengan dua cara. Cara pertama adalah dengan mengacak nomor bit dari *file host* yang digunakan untuk *embedding* pesan. Sedangkan cara kedua adalah dengan mengacak sampel *host* yang mengandung bit pesan berikutnya. Pada ELSB, letak bit pada *host* yang digunakan untuk menyisipkan pesan tidak selalu sama[4].

Pemilihan bit untuk meletakkan bit-bit pesan mempunyai aturan pada Tabel 1 sebagai berikut.

Tabel 1 Pemilihan Bit Untuk Penyisipan Bit-Bit Pesan[4]

MSB Pertama	MSB Kedua	Letak bit pesan pada *host*
0	0	LSB 3
0	1	LSB 2
1	0	LSB 1
1	1	LSB 1

Selain pemilihan letak bit untuk menyimpan bit dari pesan, dilakukan juga pemilihan *sample* yang digunakan untuk penyisipan bit pesan. Tabel 2 di bawah ini menunjukkan skema pemilihan *sample* dari *file host.*

Tabel 2 Skema Pemilihan Sampel[4]

MSB Pertama	MSB Kedua	MSB Ketiga	Sampel yang berisi bit pesan berikutnya
0	0	0	i+1
0	0	1	i+2
0	1	0	i+3
0	1	1	i+4
1	0	0	i+5
1	0	1	i+6
1	1	0	i+7
1	1	1	i+8

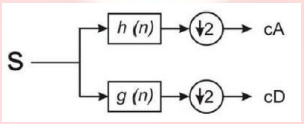
2.4 Metode Discrete Wavelet Transform[9]

Sekitar tahun 1980 pertama kali ditemukannya transformasi *Wavelet*, dimana transformasi *Wavelet* ini digunakan sebagai alternatif pengganti *Short Time Fourier Transform* untuk melakukan analisis sinyal. *Wavelet* merupakan gelombang singkat atau *small wave* yang energinya terkonsentrasi pada suatu selang waktu, yang dapat digunakan untuk analisis transien, ketidakstasioneran, dan fenomena terhadap perubahan waktu (*time varying*).

Gelombang singkat tersebut merupakan fungsi basis yang terletak pada waktu yang berbeda. *Wavelet* ini menkonsentrasikan energinya dalam ruang dan waktu sehingga cocok untuk menganalisis sinyal yang sifatnya sementara saja.

2.4.1 Dekomposisi *Wavelet*[5]

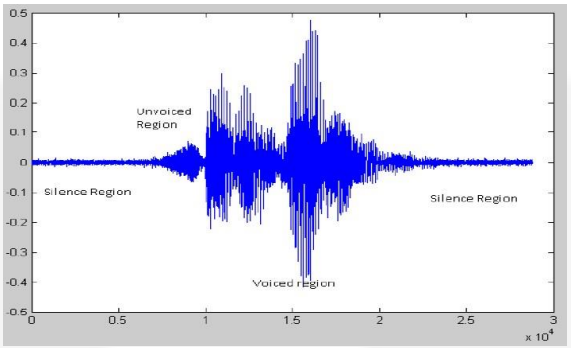
Proses transformasi pada *wavelet* pertama kali dapat diwakili dengan proses melewatkan sinyal asli ke dalam *Low Pass Filter* (LPF) dan *High Pass Filter* (HPF). LPF yang merupakan set fungsi skala menghasilkan komponen aproksimasi yang merupakan komponen sinyal berfrekuensi rendah dan berskala tinggi. Sedangkan HPF yang merupakan set fungsi *wavelet* menghasilkan komponen detail yang merupakan komponen sinyal berfrekuensi tinggi dan berskala rendah. Komponen aproksimasi dan detail yang dihasilkan melalui proses pemfilteran ini kemudian melewati proses *down sampling*. Proses ini bertujuan untuk menurunkan jumlah sampel yang dihasilkan untuk masing-masing komponen menjadi setengah dari jumlah sampel sinyal asli. Proses ini biasa dikenal dengan istilah dekomposisi *wavelet*. Proses dekomposisi *wavelet* dapat digambarkan sebagai berikut:



Gambar 1 Proses Dekomposisi *Wavelet*[5]

Proses dekomposisi dapat dilakukan berulang kali pada komponen aproksimasi, sehingga didapatkan banyak komponen resolusi yang lebih rendah dari sebuah sinyal.

2.5 Klasifikasi Sinyal Suara[1]



Gambar 2 *Silence Region, Unvoiced Region, dan Voiced Region*[1]

Pengklasifikasikan bagian-bagian atau komponen sinyal ucapan secara sederhana dibagi menjadi tiga kondisi yang berbeda, yaitu:

1) *Silence* : sinyal pada saat tidak terjadi proses produksi suara ucapan, dan sinyal yang diterima oleh pendengar dianggap sebagai bising latar belakang.
2) *Unvoiced*, keadaan pada saat *vocal cord* tidak melakukan vibrasi, sehingga suara yang dihasilkan bersifat tidak periodik atau bersifat random;
3) *Voiced*, keadaan pada saat terjadinya vibrasi pada *vocal cord*, sehingga menghasilkan suara yang bersifat kuasi periodik.

2.6 Parameter Pengujian[9]

2.6.1 *Mean Square Error* (MSE)

Mean Square Error (MSE) adalah parameter yang digunakan untuk mengukur tingkat kesalahan pada steganografi video. MSE digunakan untuk mengukur jumlah maksimal karakter yang bisa disisipkan dan mengukur tingkat kesalahan pada frame video yang telah disisipi data hiding:

$$MSE = \frac{\sum[f(\square,\square) - \square(\square,\square)]^2}{\square\square} \quad \text{.....(1)}$$

2.6.2 *Peak Signal to Noise Ratio* (PNSR)

Peak Signal to Noise Ratio (PSNR) merupakan tinjauan kualitas video secara objektif dengan mengukur kualitas steganografi video. PSNR digunkan untuk menggambarkan degradasi sebuah video akibat noising atau encoding atau kompresi atau error transmisi.

$$PSNR = 10 \times \log_{10}\left[\frac{255^2}{\square\square\square}\right] db \quad \text{.....(2)}$$

2.6.3 *Bit Error Rate* (BER)

BER (*Bit Error Rate*) adalah parameter yang digunakan untuk mengetahui tingkat kesalahan bit-bit pada steganografi video setelah diekstraksi. Jumlah bit-bit yang salah dihitung dengan membandingkan setiap video sisipan asli dengan video sisipan hasil ekstraksi.

$$BER = \frac{\sum \text{bit error}}{\sum \text{total bit}} \quad \text{.....(3)}$$

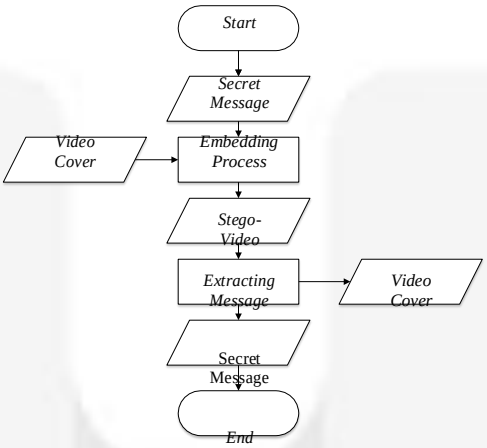
2.6.4 Mean Opinion Score (MOS)[8]

Mean Opinion Score merupakan rekomendasi ITU P.800 yang digunakan untuk mengukur kinerja dari suatu komunikasi multimedia melalui jaringan berdasarkan pandangan dari responden. responden akan memberikan penilaian dengan range angka 1-5 dimana, angka 1 berarti kualitas yang amat buruk dan angka 5 adalah kualitas yang sangat baik.

Tabel 3. Kriteria Pengujian MOS

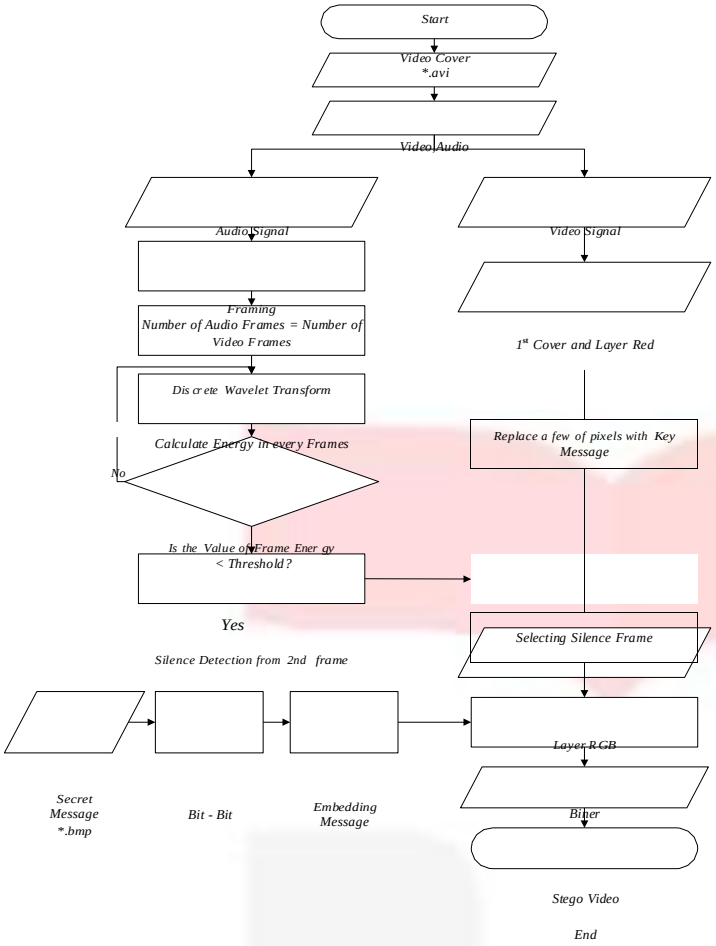
Nilai	Level Distorsi	Kualitas Video
5	Sempurna	Video memiliki kualitas yang sangat bagus, mirip dengan video asli
4	Baik	Video memiliki kualitas yang bagus.
3	Cukup	Video masih dapat dikenali, tapi terdapat kerusakan sedikit mengganggu interpretasi.
2	Kurang	Video kurang dapat dikenali, kerusakan yang ada mengganggu interpretasi.
1	Buruk	Video memiliki kualitas yang sangat rendah, hampir tidak dikenali.

2.7 Blok Diagram Sistem

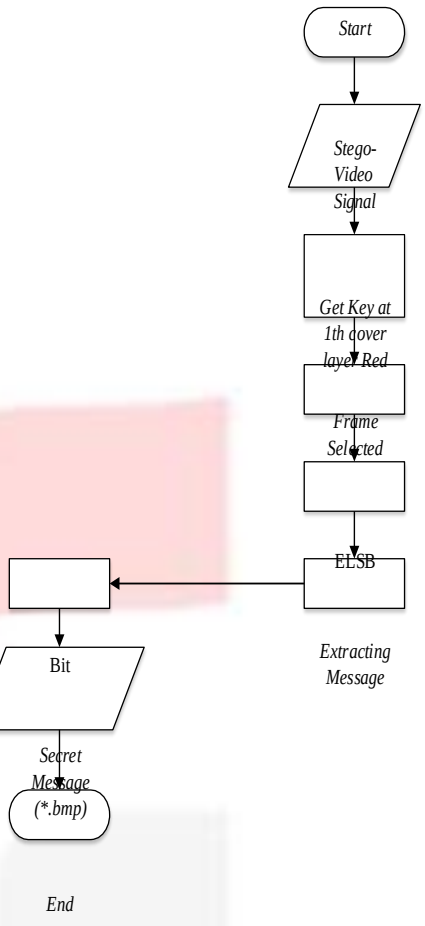


Gambar 3. Flowchart Sistem

Sistem yang dirancang pada tugas akhir ini adalah sistem steganografi dengan video sebagai *cover*. Penyisipan dilakukan di sisi pengirim dengan menyisipkan pesan rahasia berupa file citra dengan format **.bmp* ke dalam sebua *cover* yang berupa *file* video dengan format **.avi*. Keluaran dari proses penyisipan ini yaitu berupa *video steganography* dimana terdapat video yang telah disisipi pesan rahasia. Lalu *video steganography* dikirimkan ke penerima. Kemudian disisi penerima dilakukan proses ekstraksi, untuk mengembalikan pesan rahasia berupa *file* citra dengan format **.bmp* dengan jenis citra RGB.



Gambar 4 *Flowchart* Penyisipan Pesan di Sisi Pengirim



Gambar 5 *Flowchart* Proses Ekstraksi Pesan di Sisi Penerima

Berdasarkan Gambar 4, Proses *Embedding* yang dilakukan di sisi pengirim, dilakukan sebagai berikut:

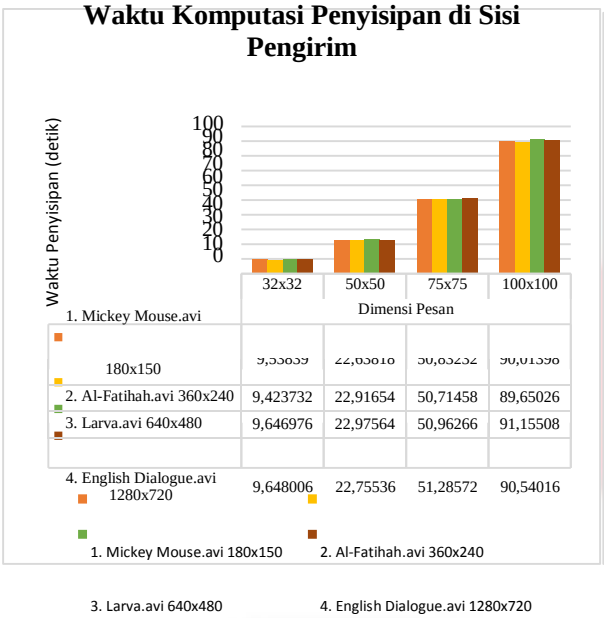
1) Sebelum dilakukan Discrete Wavelet Transform, Sinyal audio yang ada pada video dilakukan proses *Framing*. Dengan ketentuan jumlah frame audio disamakan dengan jumlah frame yang ada pada video, untuk memudahkan pendeteksian frame video.
2) *Discrete Wavelet Transform* dilakukan dengan cara men-dekomposisi sinyal audio dengan level 3, dan mother wavelet yang digunakan yaitu 'haar', yang paling sederhana dalam menganalisis sinyal audio. Hasil dari DWT kemudian dihitung energinya dengan cara mengkuadratkan masing-masing koefisien pada *subband* terpilih.
3) Daerah *silence* pada audio digunakan *threshold* amplitudo sebesar 0.0005. Jadi, *frame* yang dipilih adalah berdasarkan daerah silence yang amplitudonya dibawah *threshold* tersebut.Semakin banya daerah *silence* yang terdeteksi, maka semakin banyak pula frame yang dapat dipilih untuk menyisipkan pesan.
4) Pada sinyal video, dilakukan proses *framing* untuk membagi sinyal video menjadi beberapa frame. Tiap frame video terdiri dari tiga layer, yaitu *Red* (R), *Green* (G), dan *Blue* (B).
5) Setelah dilakukan proses *framing*, pemilihan *frame* pada penelitian ini dilakukan berdasarkan daerah *silence* pada sinyal audio yang terpilih. Sistem mencari *frame* pada sinyal video yang memiliki sinyal audio dimana amplitudonya sesuai dengan yang sudah ditetapkan pada sistem. Pada *frame* yang terpilih tersebut akan dilakukan proses penyisipan pesan rahasia. Untuk *cover* pertama di layer *Red* dilakukan proses penggantian piksel dengan informansi kunci dari pesan rahasia.
6) Setelah *frame* tersebut terpilih, maka penyisipan dapat dilakukan di semua layer RGB pada *frame* tersebut.
7) Proses pemilihan bit dilakukan setelah masing-masing *frame* terpilih pada video dipisahkan menjadi 3 layer, yaitu *Red* (R), *Green* (G), *Blue* (B). kemudian setiap layer dalam biner ditinjau MSB pertama dan MSB kedua dari *frame*. Lalu unutk pemilihan LSB dalam meletakkan bit pesan mengikuti peraturan pemilihan bit seperti pada Tabel 1.

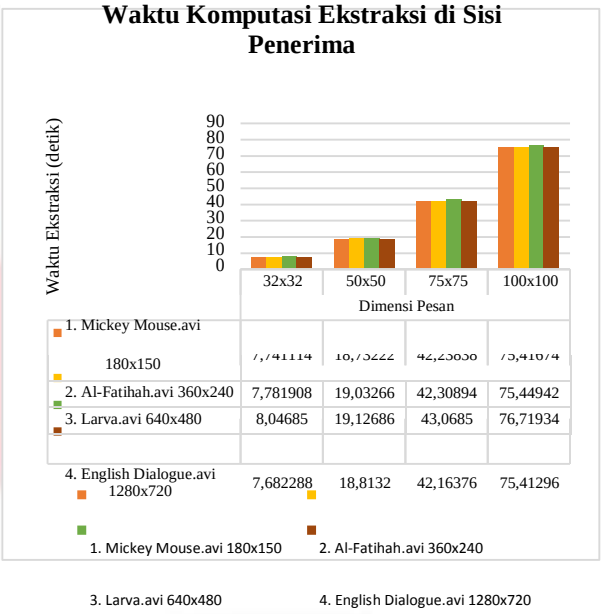
Berdasarkan Gambar 5, Proses ekstraksi merupakan proses kebalikan dari proses penyisipan. Proses ini bertujuan untuk mendapatkan pesan rahasia yang disisipkan ke dalam cover. Proses ekstraksi ini dilakukan dengan membaca kunci pada frame pertama dan layer pertama. Hal ini bertujuan untuk mengetahui informasi pesan rahasia yang disisipkan. Kemudian dilakukan proses ELSB pada frame yang tersisipi pesan berdasarkan informasi

kunci untuk mendapatkan pesan disisi penerima. Pemilihan bit dan sampel dilakukan untuk mendapatkan bit-bit pesan satu per satu mengikuti aturan ELSB seperti yang ditunjukkan pada tabel 2.1 dan 2.2. Bit-bit pesan yang telah didapatkan dipisahkan sesuai layer RGB.

3. Pembahasan

3.1 Pengaruh Panjang Pesan dan Ukuran Cover terhadap Waktu Komputasi





1. Mickey Mouse.avi 180x150	9,53839	22,63818	50,63232	90,01398
2. Al-Fatihah.avi 360x240	9,423732	22,91654	50,71458	89,65026
3. Larva.avi 640x480	9,646976	22,97564	50,96266	91,15508
4. English Dialogue.avi 1280x720	9,648006	22,75536	51,28572	90,54016

1. Mickey Mouse.avi 180x150	7,741114	18,75222	42,23838	75,41674
2. Al-Fatihah.avi 360x240	7,781908	19,03266	42,30894	75,44942
3. Larva.avi 640x480	8,04685	19,12686	43,0685	76,71934
4. English Dialogue.avi 1280x720	7,682288	18,8132	42,16376	75,41296

Gambar 6 Waktu Komputasi di Sisi Pengirim

Gambar 7 Waktu Komputasi di Sisi Penerima

Gambar 6 dan 7 merupakan waktu komputasi rata-rata yang diperlukan dalam proses penyisipan dan ekstraksi. Dalam sistem steganografi, penyisipan pesan yang berukuran 100x100 ke video cover membutuhkan waktu terlama yaitu 91,15508 detik pada video berukuran 640x480 (Larva.avi) dan untuk ekstraksi membutuhkan waktu komputasi 76,71934 detik.

Dari pengujian yang telah dilakukan, dapat dilihat bahwa semakin besar ukuran dimensi pesan yang disisipkan pada video *cover*, maka semakin lama pula waktu komputasi yang diperlukan. Begitu pula disisi penerima. Hal ini terjadi dikarenakan dalam proses penyisipan pesan maupun ekstraksi pesan pada proses steganografi dengan ukuran yang semakin besar membuat bit-bit pesan yang akan diproses semakin banyak. Namun, berdasarkan grafik diatas, ukuran *cover* video tidak berpengaruh terhadap lamanya waktu komputasi. Karena durasi masing-masing video sama. Dan juga dalam sistem steganografi, waktu ditentukan ketika proses deteksi audio dan penyisipan serta ekstraksi dilakukan.

3.2 Pengaruh Besar Dimensi Pesan dan Ukuran *Cover* Terhadap MSE dan PSNR

3.2.1 Pengaruh Ukuran *Cover* Video terhadap MSE (*Mean Square Error*)

Tabel 4 Pengaruh Ukuran Cover Video dan Besar Dimensi Pesan terhadap MSE

No.	Nama Video *Cover*	Resolusi Video	MSE			
			32x32	50x50	75x75	100x100
1.	Mickey Mouse.avi	180x150	0,03205	0,03886	0,0598881	0,0905155
2.	Al-Fatihah.avi	360x240	0,00867	0,0115	0,019237	0,0332181
3.	Larva.avi	640x480	0,01218	0,01224	0,0129959	0,0142273

3.2.2 Pengaruh Panjang Pesan dan Ukuran *Cover* Video terhadap MSE *(Mean Square Error)* Saat Semua *Silence* Tersisipi Pesan

Tabel 5 Pengaruh Ukuran *Cover* Video terhadap MSE Saat Semua *Silence* Tersisipi Pesan

No.	Nama Video Cover	Resolusi Video	Jumlah Frame *Silence*	Dimensi Pesan yang Disisipkan	MSE
1.	Mickey Mouse.avi	180x150	24	150x150	0,1560
2.	Al-Fatihah.avi	360x240	86	500x500	0,9038
3.	Larva.avi	640x480	79	800x800	0,1897

3.2.3 Pengaruh Panjang Pesan dan Ukuran *Cover* Video terhadap PSNR *(Peak Signal to Noise Ratio)*

Tabel 6 Pengaruh Ukuran *Cover* Video dan Besar Dimensi Pesan terhadap PSNR

No.	Nama Video Cover	Resolusi Video	PSNR			
			32x32	50x50	75x75	100x100
1.	Mickey Mouse.avi	180x150	63,0726	62,2355	60,3574	58,5636
2.	Al-Fatihah.avi	360x240	68,7518	67,5226	65,2894	62,9171
3.	Larva.avi	640x480	67,2751	67,2522	66,9927	66,5996

3.2.4 Pengaruh Ukuran *Cover* Video terhadap PSNR (*Peak Signal to Noise Ratio*) Saat Semua *Silence* Tersisipi Pesan

Tabel 7 Pengaruh Ukuran *Cover* Video terhadap MSE Saat Semua *Silence* Tersisipi Pesan

No.	Nama Video Cover	Resolusi Video	Jumlah Frame Silence	Dimensi Pesan yang Disisipkan	PSNR
1.	Mickey Mouse.avi	180x150	24	150x150	56,1986 dB
2.	Al-Fatihah.avi	320x240	86	500x500	48,5702 dB
3.	Larva.avi	640x480	79	800x800	55,3495 dB

3.3 Ketahanan Sistem Terhadap Serangan Noise

Tabel 8 Pengaruh *Mean* dan Variansi *Gaussian Noise* terhadap BER

Variansi	Mean		
	0	0,001	0,005
0,00000001	0	0	0,234049
0,00000002	0	0	0,234049
0,00000003	0	0	0,234049
0,00000004	0	0	0,234049
0,00000005	0	0	0,234049
0,00000006	0	0	0,234049
0,00000007	0	0,00012207	0,234049
0,00000008	0	0,00016276	0,23409
0,00000009	0	0,00020345	0,23409
0,0000001	0	0,00032552	0,233805
0,0000002	0	0,184855	0,235026
0,0000003	0,00008138	0,171102	0,233683
0,0000004	0,00044759	0,165106	0,232951
0,0000005	0,00134277	0,180054	0,236206
0,0000006	0,187052	0,184001	0,232707

Tabel 9 Pengaruh *Mean* dan Variansi *Gaussian Noise* terhadap BER Saat Semua Frame *Silence* Tersisipi Pesan

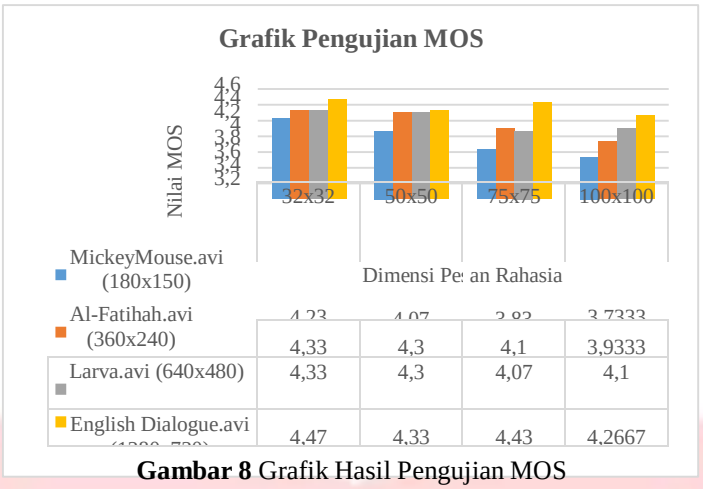
Variansi	Mean		
	0	0,1	0,5
0,00001	0,0861	0,0814	0,61339
0,1	0,86495	0,86495	0,6379696
0,3	0,86495	0,825653	0,680226
0,5	0,901899	0,84991	0,84991

Berdasarkan Tabel 8 Dan Tabel 9, besarnya serangan gaussian yang diberikan, akan sangat berpengaruh terhadap nilai BER yang dihasilkan. Semakin besar *mean* dan variansi, semakin rusak pula pesan hasil ekstraksi yang didapatkan. Hal ini terjadi karena gaussian merupakan distribusi normal dengan penyebaran acak, dimana menyebabkan titik-titik cahaya putih pada citra, sehingga mengubah piksel-piksel pada frame *stego-video* tersebut. Oleh karena itu, bit-bit yang didapat saat ekstraksi bisa jadi berbeda. Pesan hasil ekstraksi saat diberikan *noise* mudah rusak. Hanya dapat bertahan pada serangan dengan *mean* dan variansi yang sangat kecil sekali.

3.4 Pengujian Terhadap MOS

Pengujian dengan menggunakan parameter MOS digunakan untuk mengetahui kualitas video yang ter-stego dengan cover video yang memiliki ukuran 360x240, 240x180, dan 180x150. Dan panjang pesan yang berbeda-beda yaitu 32x32 piksel, 50x50 piksel, 75x75 piksel, dan 100x100 piksel.

Teknis dari pengujian MOS yaitu, 30 orang diminta untuk menonton video yang telah disisipkan pesan gambar yang berbeda-beda. Kemudian setiap orang diminta untuk menilai kualitas video tersebut, apakah video asli dan video yang ter-stego tidak terlihat beda, atau ada perbedaannya. Setiap orang diminta untuk menilai kualitas video tersebut dengan rentang dari 1 sampai dengan 5. Dengan nilai 1 menyatakan sangat buruk dan 5 sangat baik. Di bawah ini adalah grafik hasil pengujian MOS:



Gambar 8 Grafik Hasil Pengujian MOS

Berdasarkan hasil Pengujian MOS, pada grafik terlihat untuk hasil yang paling baik yaitu pada saat video cover disisipkan oleh pesan terkecil, yaitu 32x32 bit. Secara keseluruhan, hasil terendah yang diperoleh yaitu dengan nilai 3,7333 yang mengindikasikan baik. Melalui Pengujian secara subjektif, dapat disimpulkan bahwa panjang pesan yang disisipkan mempengaruhi kualitas dari video *cover*.

4. Kesimpulan

Dari hasil analisis pengujian sistem steganografi pada *frame* yang terdeteksi *silence* yang telah dilakukan, didapatkan hasil bahwa Panjang pesan sangat berpengaruh terhadap waktu komputasi. Dari penelitian yang telah dilakukan, waktu komputasi penyisipan terbesar yaitu 91,15508 dan waktu komputasi ekstraksi terbesar yaitu 76,71934. dari video cover Larva.avi (640x480) dengan besar dimensi pesan yang disisipkan sebesar 100x100 piksel. Semakin kecil ukuran cover video dan pesan yang disisipkan, maka semakin kecil pula nilai PSNR yang dihasilkan dan semakin besar nilai MSE yang dihasilkan, dan sebaliknya. Nilai MSE dan PSNR berbanding terbalik. Nilai MSE terkecil pada penelitian ini yaitu 0,00867, dan PSNR terbesar yaitu 68,7518 dB. Ukuran cover video dan banyaknya jumlah frame *silence* sangat mempengaruhi dimensi pesan yang disisipkan. Semakin besar ukuran *cover* video dan semakin banyak jumlah frame *silence* akan menyebabkan semakin banyak bit-bit pesan yang dapat disisipkan pada *cover* video. MSE terbesar yaitu 0,9038 dan PSNR terkecil yaitu 48,5702 dB dengan Al-Fatihah.avi (360x240) yang disisipkan pesan berdimensi 500x500 piksel dengan jumlah *silence frame* sebanyak 86 frame. Sistem yang telah dibuat masih sangat lemah terhadap serangan *noise*. Hal ini dapat dilihat dari hasil pengujian saat diberikan serangan *Gaussian Noise*.Dari hasil pengujian dengan MOS yang telah dilakukan, empat ukuran *cover* video yang berbeda mendapatkan nilai MOS terendah sebesar 3,733 yang mengindikasikan sistem memiliki kualitas yang baik.

Daftar Pustaka :

[1]Arry Akhmad Arman. "Proses Pembentukan dan Karakteristik Sinyal Ucapan".Departemen Teknik Elektro,ITB. Bandung.

[2] Farisah Qisthina Rekamasanti,2015. "Implementasi Analisis Video Steganografi dengan Format Video AVI Berbasis LSB (Least Significant Bit) dan SSB-4(System of Steganography Using Bit 4)". Skripsi Sarjana Telkom University Bandung : tidak diterbitkan.

[3] Hartoko, Carolus Ferdy Setiaji. 2014. "Analisis dan Simulasi Steganografi Pada Sinyal Audio Tiga Dimensi Berbasis *Enhanced Least Significant Bit*". Skripsi Sarjana Telkom University Bandung : tidak diterbitkan.

[4] Illiadi, Neng Anggi. 2015. "*Steganografi Enhanced Least Significant Bit pada Karakter Khusus Citra Tulisan Arab*". Skripsi Sarjana Telkom University Bandung : tidak diterbitkan.

[5] Moch Soleh, Ridwan. 2008. "*Denoising Rekaman Sinyal Elektrokardiogram (EKG) Menggunakan Algoritma Iterative Threshold Pada Subband Wavelet*". Skripsi Sarjana Institut Teknologi Telkom Bandung : tidak diterbitkan.

[6] Rakhi, Suresh Gawande. 2013. "*A Review on Steganography Methods*".International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering. India.

[7] Shilpa Gupta., Geeta Gujral, & Neha Aggarwal. "*Enhanced Least Significant Bit Algorithm For Image Steganography*". Manav Rachna College of Engineering Faridabad, India, 2012.

[8] ITU-R BT.500-11, *Methodology for The Subjective Assessment of The Quality of Television Pictures.*, 2002.

[9] Wahid, Muhammad Luthfi. 2015. "Analisis dan Simulasi Steganografi Video Berbasis Deteksi Band Frekuensi Menggunakan Metode Discrete Wavelet Transform".Skripsi Sarjana Telkom University Bandung : tidak diterbitkan.